Abstract

The present invention discloses a digital signature scheme based on braid group conjugacy problem and a verifying method thereof, wherein the signatory S selects three braids $x \in LB_m(l)$, $x' \in B_n(l)$, $a \in B_n(l)$, and considers braid pair(x',x) as a public key of S, braid a as a private key of S; Signatory S uses hash function h for a message M needing signature to get $y=h(M) \in B_n(l)$; generating a braid $b \in RB_{n-l-m}(l)$ randomly,t hen signing the message M with the own private key a and the braid b generated randomly to obtain $Sign(M)=a^{-1}byb^{-1}a$; a signature verifying party V obtains the public key of S,ca lculating the message M by employing a system parameter hash function h, obtaining the $y=h(M)$; judging whether $sign(M)$ and y are conjugate or not, if not,s $ign(M)$ is an illegal signature, the verification fails; if yes, $sign(M)$ is a legal signature of message M; the present invention avoids the problem of k-CSP in SCSS signature scheme of prior art, and improves the security of signature algorithm and reduces the number of braids involved and the number for conjugacy decision without reducing security, thereby improving the operation efficiency of signature.